

CLAIM AMENDMENTS

1 1. (Currently Amended) A data processing method for generating a multiplicative
2 inverse for use in determining a digital signature, the method comprising the
3 computer-implemented steps of:
4 receiving and ~~transiently~~ storing a first integer data value relating to a digital signature
5 of an electronic message;
6 ~~digitally computing~~ determining a multiplicative inverse of the first integer data value
7 modulo a prime modulus data value by computing a first quantity modulo the
8 prime modulus data value, wherein said computing includes using a modulo
9 exponentiation block;
10 wherein the first quantity ~~substantially~~ equals, modulo the prime modulus data value,
11 the first integer data value raised to a power of a second quantity;
12 wherein the second quantity is two less than the prime modulus data value; and
13 storing the multiplicative inverse in a computer hardware storage element for use in
14 determining the digital signature of the electronic message.

1 2. (Currently Amended) A method for generating a ~~digital~~ an output signal indicating a
2 multiplicative inverse of an integer data value modulo a prime modulus for use in
3 performing a particular operation, the method comprising the steps of:
4 ~~receiving~~ sending a first signal, indicating a value of the integer data value, at to a
5 base input of a modulo exponentiation block of an electronic integrated
6 circuit;
7 sending a second signal, indicating a value of the prime modulus, to a modulus input
8 of the modulo exponentiation block; and
9 sending a third signal, indicating a value of the prime modulus less two, to an
10 exponent input of the modulo exponentiation block;
11 wherein the modulo exponentiation block generates an output based on a first quantity
12 modulo a value at the modulus input; ~~and~~

13 wherein the first quantity ~~substantially~~ equals, modulo the value at the modulus input,
14 a value at the base input raised to a power of a value at the exponent input;
15 and
16 wherein the output generated by the modulo exponentiation block is stored in a
17 computer hardware storage element for use in performing a particular
18 operation that is selected from the group consisting of a digital signature
19 algorithm signing operation, a digital signature algorithm verifying operation,
20 an encryption operation for a first electronic message, and a decryption
21 operation for a second electronic message.

1 3. (Currently Amended) A method for fabricating an electronic circuit that generates an
2 output signal indicating a multiplicative inverse of an integer data value modulo a
3 prime modulus, the method comprising the steps of:
4 connecting a first register holding signals indicating a value of the integer data value
5 to a base input of a modulo exponentiation block;
6 connecting a second register holding signals indicating a value of the prime modulus,
7 to a modulus input of the modulo exponentiation block;
8 connecting a third register holding signals indicating a value of the prime modulus
9 less two, to an exponent input of the modulo exponentiation block;
10 wherein the modulo exponentiation block generates an output based on a first quantity
11 modulo a value at the modulus input; and
12 wherein the first quantity ~~substantially~~ equals, modulo the value at the modulus input,
13 a value at the base input raised to a power of a value at the exponent input.

1 4. (Currently Amended) An apparatus for generating an output signal indicating a
2 multiplicative inverse of an integer modulo a prime modulus comprising:
3 a modulo exponentiation block configured to generate the output signal based on a
4 first quantity modulo a value at a modulus input, the first quantity
5 ~~substantially~~ equal, modulo the value at the modulus input, to a value at a base
6 input raised to a power of a value at an exponent input;

7 a first input for receiving a first signal indicating a value of the integer, the first input
8 connected to the base input;
9 a second input for receiving a second signal indicating a value of the prime modulus,
10 the second input connected to the modulus input; and
11 a circuit connected to the second input configured to generate on a first output a third
12 signal indicating a value of the prime modulus less two, the first output
13 connected to the exponent input.

1 5. (Currently Amended) An apparatus for performing a particular operation for using
2 digital signatures on a network, the apparatus comprising a modulo exponentiation
3 block configured for producing a multiplicative inverse of an integer modulo a prime
4 modulus, wherein said multiplicative inverse is used in performing the particular
5 operation.

1 6. (Currently Amended) The apparatus as recited in Claim 5, ~~further comprising~~
2 wherein the apparatus has no circuitry block configured to perform an extended
3 Euclidian algorithm (EEA) and no general-purpose processor configured by
4 instructions to perform the EEA.

1 7. (Original) The apparatus as recited in Claim 5, wherein:
2 the particular operation is performed in a series of sequential computations
3 accomplished over a corresponding series of computation cycles; and
4 the apparatus further comprises connections configured to use the modulo
5 exponentiation block during a plurality of computation cycles of the series of
6 computation cycles.

1 8. (Currently Amended) The apparatus as recited in Claim 5, wherein the particular
2 operation is ~~an RSA~~ a Rivest, Shamir, and Adleman encrypting operation.

1 9. (Currently Amended) The apparatus as recited in Claim 5, wherein the particular
2 operation is ~~an RSA~~ a Rivest, Shamir, and Adleman decrypting operation.

1 10. (Original) The apparatus as recited in Claim 5, wherein the particular operation is a
2 digital signature algorithm signing operation.

1 11. (Original) The apparatus as recited in Claim 5, wherein the particular operation is a
2 digital signature algorithm verifying operation.

1 12. (Currently Amended) A computer-readable medium carrying one or more sequences
2 of instructions for generating a multiplicative inverse of an integer modulo a prime
3 modulus for use in performing a particular operation, which instructions, when
4 executed by one or more processors, cause the one or more processors to carry out the
5 steps of:
6 sending data indicating a value of the integer as an base input to a modulo
7 exponentiation function;
8 sending data indicating a value of the prime modulus as an modulus input to the
9 modulo exponentiation function; and
10 sending data indicating a value of the prime modulus less two as an exponent input of
11 the modulo exponentiation function,
12 wherein
13 the modulo exponentiation function generates an output based on a first
14 quantity modulo the modulus input, ~~and~~
15 the first quantity ~~substantially~~ equals, modulo the modulus input, the base
16 input raised to a power of the exponent input; and
17 the output generated by the modulo exponentiation function is used in
18 performing a particular operation that is selected from the group
19 consisting of a digital signature algorithm signing operation, a digital
20 signature algorithm verifying operation, an encryption operation for a
21 first electronic message, and a decryption operation for a second
22 electronic message.

1 13. (Original) The computer-readable medium recited in Claim 12, wherein the
2 exponentiation function sends the base input, the modulus input and the exponent
3 input to a special-purpose block of circuitry configured to perform modulo
4 exponentiation.

1 14. (New) A computer-readable medium carrying one or more sequences of instructions
2 for generating a multiplicative inverse for use in determining a digital signature,
3 which instructions, when executed by one or more processors, cause the one or more
4 processors to carry out the steps of
5 receiving and storing a first integer data value relating to a digital signature of an
6 electronic message;
7 determining a multiplicative inverse of the first integer data value modulo a prime
8 modulus data value by computing a first quantity modulo the prime modulus
9 data value, wherein said computing includes using a modulo exponentiation
10 block;
11 wherein the first quantity equals, modulo the prime modulus data value, the first
12 integer data value raised to a power of a second quantity;
13 wherein the second quantity is two less than the prime modulus data value; and
14 storing the multiplicative inverse in a computer hardware storage element for use in
15 determining the digital signature of the electronic message.

1 15. (New) An apparatus for generating a multiplicative inverse for use in determining a
2 digital signature, the method comprising the computer-implemented steps of:
3 means for receiving and storing a first integer data value relating to a digital signature
4 of an electronic message;
5 means for determining a multiplicative inverse of the first integer data value modulo a
6 prime modulus data value by computing a first quantity modulo the prime
7 modulus data value, wherein said computing includes using a modulo
8 exponentiation block;

9 wherein the first quantity equals, modulo the prime modulus data value, the first
10 integer data value raised to a power of a second quantity;
11 wherein the second quantity is two less than the prime modulus data value; and
12 means for storing the multiplicative inverse in a computer hardware storage element
13 for use in determining the digital signature of the electronic message.

- 1 16. (New) An apparatus for generating a output signal indicating a multiplicative inverse
2 of an integer data value modulo a prime modulus for use in performing a particular
3 operation, the apparatus comprising:
4 means for sending a first signal, indicating a value of the integer data value, to a base
5 input of a modulo exponentiation block of an electronic integrated circuit;
6 means for sending a second signal, indicating a value of the prime modulus, to a
7 modulus input of the modulo exponentiation block; and
8 means for sending a third signal, indicating a value of the prime modulus less two, to
9 an exponent input of the modulo exponentiation block;
10 wherein the modulo exponentiation block includes means for generating an output
11 based on a first quantity modulo a value at the modulus input;
12 wherein the first quantity equals, modulo the value at the modulus input, a value at the
13 base input raised to a power of a value at the exponent input; and
14 wherein the output generated by the modulo exponentiation block is stored in a
15 computer hardware storage element for use in performing a particular operation
16 that is selected from the group consisting of a digital signature algorithm
17 signing operation, a digital signature algorithm verifying operation, an
18 encryption operation for a first electronic message, and a decryption operation
19 for a second electronic message.